

**Приходько Юлія Едуардівна,
Асатрян Крістіна Суренівна**

студенти 4 курсу цивільної та господарської юстиції
Національного університету “Одеська юридична академія”

КІБЕРЗЛОЧИННІСТЬ ЯК ОДИН ІЗ НАЙБІЛЬШ ПРОГРЕСИВНИХ ВИДІВ СУЧАСНОЇ ЗЛОЧИННОСТІ

Свого часу Білл Гейтс зазначав, що в майбутньому на ринку будуть присутні тільки два види компаній: ті, хто в Інтернеті і ті, хто вийшов з бізнесу [1].

Варто сказати, що це майбутнє вже настало, оскільки бізнес масово починає переносити свою діяльність у Всесвітню павутину, розуміючи те, що мережа Інтернет допомагає суттєво мінімізувати значний обсяг витрат на ведення господарської діяльності, розширити клієнтську базу та значно збільшити прибутки в ході своєї діяльності.

Однак, поряд із цим виникає і масово розвивається кіберзлочинність у зв'язку із величезним обігом коштів у даній сфері суспільних відносин.

Відповідно до п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 р. кіберзлочини у вузькому та широкому сенсі. Кіберзлочини у вузькому сенсі («комп'ютерні злочини») – будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних, кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) – будь-яке протиправне діяння, що вчинюється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [2].

Станом на сьогодні кіберзлочинність є одним з найбільш активно прогресуючих видів злочинності. Великими темпами розвиваються нові види кіберзлочинів, а також суттєво збільшується їх кількісне значення та територія поширення. Для прикладу, Н. Мішук зазначає, що за даними фахівців США, розмір збитків від кіберзлочинності кожного року зростає в середньому на 35% порівняно з попереднім. Однією з причин такого стрімкого розвитку є саме кількість коштів, яку можна отримати при вчиненні кіберзлочину. Середня кількість збитків від кіберзлочину у світі становить приблизно 560 тисяч доларів, тоді як при звичному пограбуванні банку – приблизно 20 тисяч доларів [3, с. 174].

Щодо особи потерпілого, то у звіті компанії Norton щодо статистики стану кіберзлочинності та кібербезпеки у 2017 році зазначається, що існує загальна тенденція, при якій особи занадто впевнені в тому, що вони перебувають у безпеці знаходячись у мережі Інтернет, але хакери

демонструють зворотнє. Так лише за 2017 рік було отримано злочинним шляхом 172 мільярди доларів із 978 мільйонів споживачів з 20 різних країн.

В усьому світі жертви кіберзлочинів характеризуються зазвичай тим, що вони використовують безліч пристроїв як вдома, так і поза ним, але не дотримуються елементарних правил безпеки при користуванні мережею Інтернет.

Серед основних помилок користувачів виокремлюються такі як: використання одного і того ж паролю у кількох облікових записах, надсилання паролів чи даних банківських карток незахищеними каналами зв'язку, невикористання Проху-сервісів або VPN-сервісів у момент підключення до спільних безкоштовних точок WiFi-доступу до мережі Інтернет, в ході якої особисті дані користувача можуть вилучені сторонніми особами тощо.

Тільки у 2017 році у США 143 мільйони споживачів стали жертвами кіберзлочинів – це більше половини дорослого населення цієї країни. Втрати склали приблизно 20 мільярдів доларів [4].

З огляду на це, можемо підсумувати, що кіберзлочинність є одним із найбільш прогресивних видів злочинності на сучасному етапі розвитку суспільства, що породжено значним поширенням використання мережі Інтернет у різних сферах суспільного життя та низькою захищеністю персональних даних користувачів Всесвітньої павутини. Саме тому, якщо будь-яка особа бажає вберегти власний бізнес, свої персональні дані та персональні дані компанії, мінімізувати можливості несанкціонованого стягнення своїх активів сторонніми особами, то така особа має докласти усіх зусиль щоб попередити та зупинити такі дії. На нашу думку, основними засобами захисту особи можуть стати різні перевірені сервіси зберігання інформації, які допоможуть зберігати дані щодо ключів та паролів (наприклад, додаток Wallet від компанії Apple Inc.), а також VPN-сервіси (наприклад, додаток VPN Unlimited від компанії KeepSolid Inc.), які надають змогу використання іншого сервера для підключення до мережі Інтернет, що мінімізує ризики вилучення інформації сторонніми особами при підключенні через точки WiFi-доступу, особливо через безкоштовні громадські точки доступу.

Список використаних джерел

1. Гейтс Б. Бизнес со скоростью мысли / Билл Гейтс. — Изд. 2-е, испр. — М. : ЭКСМО-Пресс, 2001. — 480 с.
2. A/CONF.187/15 // Доповідь Десятого конгресу ООН із запобігання злочинності й поведженню з правопорушниками (Відень, 10–17 квіт. 2000 р.). — Режим доступу: <http://undocs.org/A/CONF.187/15>.
3. Мішук Н. Кіберзлочинність як загроза інформаційному суспільству / Н. Мішук // Вісник Львівського університету. — Серія економічна. — 2014. — Випуск 51. — С. 173–179.

4. Consumers' Overconfidence Helps Hackers Up the Ante and Steal \$172 Billion in 2017 [Електронний ресурс]. – Режим доступу: https://www.symantec.com/about/newsroom/press-releases/2018/symantec_0122_01.

Ключові слова: кіберзлочинність, кіберзлочини, транснаціональні злочини, інформаційні технології, мережа Інтернет.

Науковий керівник: *к.ю.н., доцент Дикий О. В.*

Рибчук Анастасія Сергіївна

студентка 1-го курсу магістратури Інституту кримінальної юстиції
Національного університету «Одеська юридична академія»

ЛЕГАЛІЗАЦІЯ «ЛЕГКИХ» НАРКОТИКІВ ЯК ЗАСІБ ПРОТИДІЇ ТРАНСНАЦІОНАЛЬНОМУ НАРКОБІЗНЕСУ: ЗАРУБІЖНИЙ ДОСВІД

Наркоманія являє собою глобальну проблему, якій притаманний міжнародний характер. Підвищення попиту на наркотики, надвисокі прибутки від їх виготовлення і розповсюдження, корупція державних службовців і розширення організованої злочинності створюють умови для розвитку наркобізнесу, як різновиду транснаціональної злочинності.

Суттєве погіршення ситуації у сфері обігу наркотиків в Україні, помітне зростання пов'язаної з цим злочинності, а також посилення зв'язків вітчизняних наркототорговців з зарубіжним наркотичним бізнесом значно актуалізували проблему боротьби з незаконним обігом наркотичних засобів та психотропних речовин [1]. Зважаючи на це в Україні все частіше постає питання про можливу легалізацію так званих «легких» наркотиків. Спроба впровадити такий підхід спирається на досвід таких держав, як Польща, Німеччина, Голландія, які використовують ліберальний метод протидії наркоманії [2, с. 163–165].

Прихильники легалізації наркотичних засобів в Україні аргументують свою позицію тим, що залежна особа стає злочинцем лише в тому випадку, якщо йому наркотик недоступний, і в результаті він змушений йти на злочин, щоб його добути. Таким чином легалізація наркотиків знизить рівень злочинності, що пов'язана з їх споживанням. Проте, як свідчить практика, будь-яке короткочасне скорочення кількості арештів після скасування законів про споживання наркотиків швидко сходить нанівець, у міру того, як збільшується їх споживання.

Міністерство юстиції США встановило, що злочинці під впливом наркотиків здійснюють в шість разів більше вбивств, в чотири рази більше нападів і майже в півтора рази більше пограбувань в порівнянні